Lebeau TP Durcissement sécurité AD et serveur + Laps BTS SIO2

Mathéo

Intro:

Dans ce tp nous allons améliorer la sécurité de notre serveur AD ainsi que notre windows serveur et on finira avec l'installation de windows Laps. Ces mesures visent à améliorer la sécurité pour se défendre de potentielles attaques malveillantes.

Commençons avec le Durcissement et Sécurité Windows Server. Rendons-nous sur l'ad et on va réactiver tous les pare-feu désactivés

Pare-feu Microsoft Defender Public : Actif

Windows

(I) Pare-feu et protection du

Qui et ce qui peut accéder à vos réseaux.

Réseau avec domaine Le pare-feu est activé.

Réseau privé Le pare-feu est activé.

Se Réseau public (actif) Le pare-feu est activé.

Puis il faut effectuer les mises à jour et cocher les cases suivantes



*Votre organisation gère certain

Options de mise à jour

Recevoir les mises à jour d'autre



Téléchargez les mises à jour via (



Redémarrez cet appareil dès que l'appareil doit être allumé et bra

Et dans les paramètres de l'antivirus directement cocher toutes les cases de protection.



Ensuite comme notre serveur n'utilise pas d'imprimante on va désactiver et arrêter le spouleur d'impression dans les services.

🤐 SMP de l'Espace de stocka	g	Servic		Manuel	
Spouleur d'impression		Ce ser.	En cours d'	Automatic	
🏟 Station de travail		Crée	Démarrer		
🎑 Stockage des données utilis		Gère I	Arrêter		
🖾 Stratégie de retrait de la cart		Autor	Suspendre		
C:\Windows\System32\spoolsv.exe					
Type de démarrage :	Automatique		~		
	Auto Auto Man Dés	omatique (omatique uel activé	début différé)		

Il faut vérifier aussi à bien désactiver la fonctionnalité smb 1.0 obsolète.



On va ensuite par sécurité activer les clichés instantanés sur notre disque C.

C:\	Désactivé	2
Activer		Désactiver

On peut également les planifier si besoin par jours

ect.

Volume	Heure de la procha	Par
\\?	Désactivé	0
🕞 C:\	10/12/2024 12:00	2

ement avec BitLocker dans les fonctionnalités.

	Activer	Dés	activer		
-	Clichés instantane	és du volume sélection	né		
	10/12/2024 09	:56	r BitLock	er sur le disque	
	cpingiei a	Acces taplue			
	🎈 Activer Bit	Locker			

Puis il faudra simplement choisir le répertoire où l'on enregistrera le fichier correspondant à la clé de récupération et enfin il faudra choisir le dernier type de chiffrement.

Deuxième partie pour notre tp on va passer à la Sécurité contrôleur de domaine Active Directory.

On va se rendre dans le centre d'administration.



Et on active la corbeille ce qui nous permettra de rétablir les éventuelles suppressions accidentelles.

Ensuite on se rend dans l'outil d'administration suivant.

```
Modification ADSI
```

Puis sur action on fait connexion et la fenêtre suivante apparaît.

	Paramètres de connexion X				
1	Nom : Contexte d'attribution de noms par défaut				
e	Chemin d'accès : LDAP://SRV-AD-DNS-ML.japon.local/Contexte d'attribution				
ļ	Point de connexion				
l l	$\bigcirc \underset{n \text{ oms}}{\text{Sélectionnez ou entrez un nom unique ou un contexte d'attribution de noms :}}$				
4	×				
d	Sélectionnez un contexte d'attribution de noms connu :				
li	Contexte d'attribution de noms par défaut $\qquad \lor$				
Ordinateur					
	Sélectionnez ou entrez un domaine ou un serveur : (Serveur Domaine [:port])				
	× .				
Par défaut (le domaine ou le serveur auquel vous vous êtes connecté)					
	Utiliser le chiffrement SSL				
	Avancé OK Annuler				

Et on fera juste OK sans rien toucher.

msDS-ExpireP	asswordsOnSmartCardOnlyAccounts	TRUE	
Éditeur d'attribut	s de type Entier		×
Attribut :	ms-DS-MachineAccountQuota		
Valeur :			
0			
Effacer	0	K /	Annuler

Puis dans les propriétés du domaine dans l'éditeur d'attribut on va chercher

Et en double cliquant dessus on le mettra à 0. Ce paramètre à 0 fera qu'uniquement les admins pourront mettre des machines au domaine.

On va maintenant se rendre dans l'ad et supprimer les droits de rétrocompatibilité avant windows 2000



Ensuite dans le gestionnaire de stratégie de groupe.

On va Désactiver NTLMv1 et NTLMv2 qui sont des protocoles parfois utilisés mais dangereux.

 Stratégie desactiver NTLM (SRV-AD-DNS-MLJAP) Configuration ordinateur Stratégies Paramètres du logiciel Paramètres Windows Stratégie de résolution de noms Scripts (démarrage/arrêt) Paramètres de sécurité 	Stratégie Fériphériques : ne permettre l'accès aux disquettes qu'aux utilisateurs connectés localement Périphériques : permettre le formatage et l'éjection des médias amovibles Sécurité réseau : conditions requises pour la signature de client LDAP Sécurité réseau : forcer la fermeture de session quand les horaires de connexion expirent Sécurité réseau : ne pas stocker de valeurs de hachage de niveau LAN Manager sur la prochain Sécurité réseau : niveau d'authentification LAN Manager	Paran Non o Non o Non o Non o Non o
 Paramètres de sécurité Stratégies de comptes Stratégies locales Stratégie d'audit Attribution des droits utilisa Options de sécurité 	 Sécurité réseau : niveau d'authentification LAN Manager Sécurité réseau : sécurité de session minimale pour les clients basés sur NTLM SSP (y compris R Sécurité réseau : sécurité de session minimale pour les serveurs basés sur NTLM SSP (y compris Sécurité réseau : Autoriser le retour à des sessions NULL avec SystèmeLocal Sécurité réseau : autoriser les demandes d'authentification PKU2U auprès de cet ordinateur po Sécurité réseau : Autoriser Système local à utiliser l'identité de l'ordinateur pour NTLM 	Non o Non o Non o Non o Non o
> journal des événements	🛛 📓 Sécurité réseau : Configurer les types de chiffrement autorisés pour Kerberos	Non o



Puis retournons sur l'ad et on va faire quelque manipulation pour veiller a la bonne sécurité de l'utilisateur kerberos qui sert a l'authentification.

Et on va lancer le powershell et faire quelques commandes.



For the AD forest to be targeted, please provide the FQDN or press [ENTER] for the current AD forest: : For the AD domain to be targeted, please provide the list nr or the FQDN or press [ENTER] for the current AD domain: :

De même.

Puis



pwdLastSet 10/12/2024 11:47:33 Paris, Madrid Le mot de passe à bien été changé on a maintenant terminé la sécurisation de l'ad et on va passer a la dernière partie avec l'installation de windows laps